23-mj-6445-MPK
23-mj-6446-MPK

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Michael Mobilia, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent with the Federal Bureau of Investigation and have been since July 2019. During this time, I have received training at the FBI Academy located in Quantico, Virginia, to include training on investigative methods and training specific to counterintelligence and espionage investigations. I am currently assigned to a squad at the FBI Washington Field Office, Counterintelligence Division, where I primarily investigate counterintelligence and espionage matters. During these investigations, I have conducted or participated in witness and subject interviews, service of subpoenas, the execution of search and arrest warrants, physical surveillance, the seizure of evidence, including computer, electronic, and email evidence, as well as requested and reviewed pertinent records. Based on my experience and training, I am familiar with the requirements for the handling of classified documents and information. I am also familiar with the methods used by individuals engaged in the unlawful use or disclosure of classified information, including national defense information.

2. I am currently investigating Jack Douglas Teixeira ("TEIXEIRA") for the Unauthorized Removal, Retention, and Transmission of Classified Documents or Material in violation of 18 U.S.C. §§ 793(b)-(e) and 1924, as well as the Destruction, Alteration and Falsification of Records in a Federal Investigation in violation of 18 U.S.C. § 1519 ("the SUBJECT OFFENSES").

3. I make this affidavit in support of an application for a search warrant for information associated with two cellular telephones assigned call numbers [redacted] and [redacted], ("the SUBJECT PHONES"), that is stored at premises controlled by Verizon

Wireless ("Verizon"), a wireless telephone service provider headquartered at 180 Washington Road in Bedminster, New Jersey. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. § 2703(c)(1)(A) to require Verizon to disclose to the government copies of the information further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review the information to locate items described in Section II of Attachment B.

4. I also make this affidavit in support of an application for a warrant to search TEIXEIRA's person for deoxyribonucleic acid ("DNA") in the form of one or more buccal (oral) swabs. Based upon the information set forth below, there is probable cause to believe that TEIXEIRA's DNA contains evidence of the crimes specified in this affidavit.

5. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrants and does not set forth all my knowledge about this matter.

PROBABLE CAUSE

6. On April 17, 2023, FBI Special Agent Victoria Horne submitted an affidavit in support of an application for a search warrant to Discord (M.J. No. 23-mj-4301-DHH). I have reviewed that affidavit and a copy of it is attached. *See* Exhibit 1. Based on conversations with Special Agent Horne and my own participation in the investigation, I believe that the April 17,

2023, affidavit is accurate and I seek to incorporate the facts set forth in that affidavit herein.[1] To the extent the affidavit provides information relevant to the issue of probable cause, I have not repeated the information below but have, instead, updated and supplemented the information to include the results of the investigation to date.

7. As described in Exhibit 1, the FBI has been investigating the unauthorized disclosure of classified national defense information by TEIXEIRA on a social media platform called Discord. A grand jury sitting in the District of Massachusetts recently returned a six-count indictment against TEIXEIRA charging him with the Willful Retention and Transmission of National Defense Information in violation of 18 U.S.C. § 793(e). *See* Case No. 23-cr-10159-IT at ECF No. 48. The FBI investigation of TEIXEIRA is ongoing.

8. As part of its investigation of TEIXEIRA, the FBI has obtained (through three successive search warrants) records from Discord concerning TEIXEIRA's Discord user account. These records include, among other things, the content of communications sent and received by TEIXIERA concerning the unauthorized disclosure of classified national defense information. Some of these communications date back to January 2022. For example, between January 15 and January 17, 2022, TEIXEIRA and another Discord user (whose account has since been deleted) had the following conversation:

TEIXEIRA: sry it took so long to respond work was a bitch today
TEIXEIRA: and this whole week too
Deleted User: What happened?
TEIXEIRA: Sleep schedule got raped

[1] In paragraph 16 of the Horne Affidavit, it was noted that TEIXEIRA currently holds a security clearance. I have confirmed with the Department of Defense that Teixeira has now been declared ineligible for a clearance.

Deleted User: That's the military for you
Deleted User: Russia?
TEIXEIRA: I do have quite a bit to tell

TEIXEIRA then proceeded to send the user multiple messages that contain presumptively classified information.[2]

9. Similarly, on February 20, 2022, TEIXEIRA engaged in the following conversation with another Discord user in which he again disclosed presumptively classified information:

TEIXEIRA: Yo
TEIXEIRA: You live near [foreign city] yeah?
User: yeah
User: village next to it
User: why ?
TEIXEIRA: Good
TEIXEIRA: There will be a wave of niggers from [city in Ukraine] soon
TEIXEIRA: When it happens
User: so never ?
TEIXEIRA: I'll elaborate more when I get home
TEIXEIRA: [PRESUMPTIVELY CLASSIFIED]
TEIXEIRA: That's what I was told and I did more digging and that's what more and more people are saying

10. In addition, the investigation of TEIXEIRA has revealed that he obtained his TS/SCI clearance on July 7, 2021, and that he began accessing Intel Link in August 2021. Furthermore, USG Agency 1 has also confirmed that TEIXEIRA used his classified government network to conduct keyword searches for classified information as early as November 2021. In

[2] The information is described as "presumptively" classified because it does not appear in the form of an official government document with classified markings, but rather as text typed by TEIXEIRA into Discord. Nonetheless, the information is consistent with classified information maintained by various U.S. government agencies, to which TEIXEIRA would have had access by virtue of his employment with USANG.

light of these facts, there is probable cause to believe that TEIXEIRA's unlawful dissemination of classified information on Discord was ongoing as of January 2022.

11. The records produced by Discord also contain communications evidencing TEIXEIRA's attempts to avoid being identified by law enforcement. For example, on April 6, 2023, after being made aware that some of the classified materials he posted on Discord has been further disseminated (and approximately one week before his arrest), TEIXEIRA engaged in this exchange with another Discord user:

User:	i think your thingies got passed along
User:	seeing pro rus telegram with them
TEIXEIRA:	Which ones?
User:	i screenshotted one can i send?
TEIXEIRA:	Sure
...	
User:	is it actually one of them btw?
TEIXEIRA:	Not commenting
User:	aight
User:	ima delete it too
User:	did you share them outside of abis?
TEIXEIRA:	I think I'm done talking about this
User:	ok
TEIXEIRA:	Permanently
User:	sorry if I pushed you here
TEIXEIRA:	It's fine
TEIXEIRA:	Just letting u know I'm leaving the server
TEIXEIRA:	Don't make a huge deal of it

Shortly thereafter, the Defendant received a password reset link from Discord followed by an email indicating that his password has been changed. The Defendant changed his account username several minutes later.

12. The next day, April 7, 2023, TEIXEIRA instructed another Discord user to delete all conversations stored in the Discord server, stating, "ban me and delete all messages." When that user told him that "it only goes to past 7 days," TEIXEIRA's response was, "[f]uck Alr nvm

[alright, never mind] . . . Just find stuff from Feb 2022 in civil discussion and delete it during your free time." He also told that user, "[i]f anyone comes looking, don't tell them shit," and he asked the user to pass this message on to others. Once again, TEIXEIRA changed his account username and profile picture.

13. According to a former co-worker of TEIXEIRA's, on April 12, 2023 (the day before TEIXEIRA was arrested), TEIXEIRA was reading the Bible at work and told the co-worker that his cell phone fell out of his vehicle while driving and was subsequently struck by a "semi truck." The co-worker believed that TEIXEIRA's old phone (the one TEIXEIRA said had been run over by a truck) was an iPhone 8, and that TEIXEIRA was in possession of a new phone at work on April 12, 2023.

14. On April 13, 2023, the FBI arrested TEIXEIRA and searched his residence located at [redacted] (hereinafter "the residence") pursuant to a judicially authorized search warrant. *See* M.J. No. 23-mj-4242-DHH. Among other areas, the warrant authorized the search of the grounds surrounding the residence, including all "trash areas." *Id.* at Attachment A.

15. During the search of the residence, FBI investigators located a Motorola cell phone inside the residence. The phone number associated with this phone is [redacted] (*i.e.*, one of the SUBJECT PHONES). Records produced by Verizon in response to legal process indicate that TEIXEIRA is the phone's user, and that the phone was activated on April 10, 2023.[3]

[3] According to records produced by Verizon, the other SUBJECT PHONE – [redacted] – was also used by TEIXEIRA throughout 2022 until approximately April 8, 2022.

16. At the time of the search on April 13th, there was a large, commercial-sized dumpster located at the residence along the driveway close to Maple Street.[4] Inside the dumpster, among other things, investigators located numerous electronic devices and components. These devices and components were discovered on top of the other items inside the dumpster — the dumpster was more than half full of cardboard and other trash — suggesting they had been placed there relatively close in time to the search. As described in paragraph 22 of Exhibit 1, the FBI surveilled TEIXEIRA at the residence on the morning of April 13, 2023, several hours prior to his arrest and the search of the dumpster.

17. The devices and components found inside the dumpster included, among other things, an iPad, an Acer brand laptop computer, an Xbox One gaming console, a CyberPower brand gaming keyboard[5], and a GoPro camera. The iPad, in particular, appeared to have been intentionally destroyed. As depicted below, the iPad's screen was removed and shattered, and many of the internal components were damaged. Because it was so heavily damaged, the FBI has not been able to recover the content of the iPad.

---

[4] The dumpster was like those used by many commercial establishments to dispose of trash. In fact, the residence included a floral design business – including greenhouses and a retail space – owned and operated by TEIXEIRA's mother. This business appeared to be operational as of the date of the search.

[5] Importantly, a similar keyboard appears in the background of several photographs of classified documents posted to the Internet that have since been located by FBI. Insofar as this keyboard can be linked to TEIXEIRA, therefore, it would tend to establish that he was the person who posted the classified documents to the internet in the first instance.

iPad

18. In addition, the remnants of a computer tower — primarily the outer shell of the tower, including the fans — were also located in the dumpster, but the electronic components of the tower that would store data, such as the hard drive, had been removed and have not been located.

PROBABLE CAUSE TO BELIEVE THAT THE PERSON OF TEIXEIRA CONTAINS EVIDENCE OF THE SUBJECT OFFENSES

19. After the search on April 13th, the CyberPower brand gaming keyboard found in the dumpster outside TEIXEIRA's home in [redacted] (the "Keyboard") was submitted to the FBI Forensic Laboratory in Quantico, Virginia for DNA and fingerprint analysis. Three swabs taken from the Keyboard were found to contain male DNA originating from a single individual. This DNA evidence has been preserved by the FBI Forensic Laboratory and is suitable for

comparison to known DNA profiles. In addition, the Keyboard was found to contain several latent fingerprints, analysis of which indicates are a match to TEIXEIRA's fingerprints.

20. I know from my training and experience, and from speaking with other law enforcement agents and DNA experts, that is it possible to compare a DNA profile found on a piece of evidence (a computer keyboard, for example) to a known DNA profile from a specific, identified person in order to determine whether that person contributed his or her DNA to the piece of evidence. I know that a match between DNA found on a piece of evidence and a known DNA profile from a specific individual generally establishes a strong likelihood that the individual contributed his or her DNA to the piece of evidence. I also know from my training and experience that obtaining a sample of DNA material from an individual for comparison purposes is not an intrusive process: it merely entails swabbing the inside of the person's cheek for several seconds.

21. Obtaining a sample of TEIXEIRA's DNA will allow investigators to determine whether TEIXEIRA's DNA matches the DNA profile from the Keyboard found in the dumpster outside of the residence. Such evidence may reveal, for example, whether TEIXIERA used the keyboard and the other devices and components found near the keyboard, whether he was the person who disposed of these items in the dumpster, and (if so) approximately when he placed them there. Insofar as the keyboard was found near the iPad (which was shattered), the Acer computer, and the partial computer tower (which appears to have been dismantled), such evidence is also relevant to whether TEIXIERA is responsible for destroying, dismantling, and/or manipulating other devices found in the dumpster. Lastly, insofar as a similar or identical keyboard appears in photos of documents containing classified material posted to the internet, such evidence is also relevant to whether TEIXEIRA was the person who posted the photos to the internet in the first instance.

22. There is probable cause to believe, therefore, that TEIXEIRA's DNA constitutes and contains evidence of the SUBJECT OFFENSES, and it is hereby requested that a warrant issue requiring TEIXEIRA to provide a DNA sample in the form of one or more buccal swabs. As of the date of this affidavit, TEIXEIRA is incarcerated at the Plymouth County House of Corrections in Plymouth, Massachusetts. There is probable cause to believe, therefore, that TEIXEIRA can be found in the District of Massachusetts.

PROBABLE CAUSE TO BELIEVE THAT THE RECORDS OF VERIZON CONTAIN EVIDENCE OF THE SUBJECT OFFENSES

23. As described above, records produced by Verizon to the FBI in response to legal process indicate that TEIXEIRA is the user / subscriber of the SUBJECT PHONES and that Verizon is the provider for both phones.

24. In my training and experience, I have learned that Verizon is a company that provides cellular telephone access to the general public. I also know that providers of cellular telephone service have technical capabilities that allow them to collect and generate information about the locations of the cellular telephones to which they provide service, including cell-site data, also known as "tower/face information" or "cell tower/sector records." Cell-site data identifies the "cell towers" (i.e., antenna towers covering specific geographic areas) that received a radio signal from the cellular telephone and, in some cases, the "sector" (i.e., faces of the towers) to which the telephone connected. These towers are often a half-mile or more apart, even in urban areas, and can be 10 or more miles apart in rural areas. Furthermore, the tower closest to a wireless device does not necessarily serve every call made to or from that device. Accordingly, cell-site data provides an approximate location of the cellular telephone but is typically less precise than

other types of location information, such as E-911 Phase II data or Global Positioning Device ("GPS") data.

25. Based on my training and experience, I know that Verizon can collect cell-site data about the SUBJECT PHONES. I also know that wireless providers such as Verizon typically collect and retain cell-site data pertaining to cellular phones to which they provide service in their normal course of business in order to use this information for various business-related purposes.

26. Based on my training and experience, I know that Verizon also collects per-call measurement data, which Verizon also refers to as the "real-time tool" ("RTT"). RTT data estimates the approximate distance of the cellular device from a cellular tower based on the speed with which signals travel between the device and the tower. This information can be used to estimate an approximate location range that is more precise than typical cell-site data. In my training and experience, this RTT data and historical cell-site data may constitute evidence of the crimes under investigation because the data can be used to identify the approximate location of the SUBJECT PHONES' user (in this case TEIXEIRA) at a particular date and time. For example, the data could be used in this case (along with other evidence) to determine TEIXEIRA's whereabouts when classified information was posted on Discord, or whether TEIXEIRA was at or near Otis Air National Guard Base when certain classified documents were accessed on classified systems. Likewise, this evidence could be used to determine the veracity of TEIXIERA's claim that his cell phone was accidentally run over by a truck prior to his arrest.

27. Based on my training and experience, I know that wireless providers such Verizon typically collect and retain information about their subscribers in their normal course of business. This information can include basic personal information about the subscriber, such as name and address, and the method(s) of payment (such as credit card account number) provided by the

subscriber to pay for wireless telephone service. I also know that wireless providers such as Verizon typically collect and retain information about their subscribers' use of the wireless service, such as records about calls or other communications sent or received by a particular phone and other transactional records, in their normal course of business. In my training and experience, this information may constitute evidence of the crimes under investigation because the information can be used to identify the SUBJECT PHONES' user or users and may assist in the identification of co-conspirators and/or victims.

AUTHORIZATION REQUEST REGARDING VERIZON

28. Based on the foregoing, I request that the Court issue the proposed search warrant to Verizon, pursuant to 18 U.S.C. § 2703(c) and Federal Rule of Criminal Procedure 41.

29. I further request that the Court direct Verizon to disclose to the government any information described in Section I of Attachment B that is within its possession, custody, or control. Because the warrant will be served on Verizon, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

Respectfully submitted,

/s/ Michael Mobilia

Michael Mobilia
Special Agent
Federal Bureau of Investigation

Sworn to telephonically on September 26, 2023.

M. Page Kelley
CHIEF UNITED STATES MAGISTRATE JUDGE

Exhibit 1

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MASSACHUSETTS

IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH USER ID 7[redacted], USER ID [redacted], AND USER ID [redacted] THAT IS STORED AT PREMISES CONTROLLED BY DISCORD, INC.	M.J. No. 23-MJ-4301-DHH M.J. No. 23-mj-4302-DHH ***FILED UNDER SEAL***

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Victoria Horne, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with certain accounts that is stored at premises owned, maintained, controlled, or operated by Discord, Inc. (hereinafter "Discord"), an electronic communications service/remote computing service provider headquartered at 444 De Haro Street, San Francisco, California. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Discord to disclose to the government records and other information in its possession pertaining to the subscriber or customer associated with the accounts, including the contents of communications.

2. I am a Special Agent with the Federal Bureau of Investigation and have been since April 2021. As a Special Agent, I have received training at the FBI Academy located in Quantico, Virginia, including training on investigative methods and training specific to counterintelligence and espionage investigations. I am currently assigned to a squad at the FBI

Washington Field Office, Counterintelligence Division, where I primarily investigate counterintelligence and espionage matters. During the course of these investigations, I have conducted or participated in witness and subject interviews, service of subpoenas, the execution of search and arrest warrants, physical surveillance, the seizure of evidence, including computer, electronic, and email evidence, as well as requested and reviewed pertinent records. Based on my experience and training, I am familiar with the requirements for the handling of classified documents and information. I am also familiar with the methods used by individuals engaged in the unlawful use or disclosure of classified information, including national defense information.

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. As described more fully below, I respectfully submit that there is probable cause to search the information described in Attachment A for evidence of these crimes further described in Attachment B, for evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 793(b), (c), (d), and (e) and/or 18 U.S.C. § 1924 (the "SUBJECT OFFENSES").

JURISDICTION

5. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711, 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

PROBABLE CAUSE

Statutory Authorities and Definitions

6. Pursuant to 18 U.S.C. § 793(b), "[w]hoever . . . copies, takes, makes, or obtains, or attempts to copy, take, make or obtain, any sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance, document, writing, or note of anything connected with the national defense" shall be fined or imprisoned not more than ten years, or both.

7. Pursuant to 18 U.S.C. § 793(d), "[w]hoever, lawfully having possession of, access to, control over, or being entrusted with any document . . . or note relating to the national defense, or information relating to the national defense which information the possessor has reason to believe could be used to the injury of the United States or to the advantage of any foreign nation, willfully communicates, delivers, transmits or causes to be communicated, delivered, or transmitted or attempts to communicate, deliver, transmit or cause to be communicated, delivered or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it on demand to the officer or employee of the United States entitled to receive it" shall be fined or imprisoned not more than ten years, or both.

8. Pursuant to 18 U.S.C. § 793(e), "[w]hoever having unauthorized possession of, access to, or control over any document . . . relating to the national defense . . . willfully communicates, delivers, transmits or causes to be communicated, delivered, or transmitted" or attempts to do or causes the same "to any person not entitled to receive it, or willfully retains the same and fails to deliver it to the officer or employee of the United States entitled to receive it" shall be fined or imprisoned not more than ten years, or both.

9. Pursuant to 18 U.S.C. § 1924, it is illegal for any officer, employee, contractor, or consultant of the United States, who, by virtue of his/her office, employment, position, or contract, becomes possessed of documents or materials containing classified information, to knowingly remove such documents or materials without authority and with the intent to retain such documents or materials at an unauthorized location.

10. Under Executive Order 13526, the unauthorized disclosure of material classified at the "TOP SECRET" level ("TS"), by definition, "reasonably could be expected to cause exceptionally grave damage to the national security" of the United States. Exec. Order 13526 § 1.2(a)(1), 75 Fed. Reg. 707, 707–08 (Jan. 5, 2010). The unauthorized disclosure of information classified at the "SECRET" level ("S"), by definition, "reasonably could be expected to cause serious damage to the national security" of the United States. Exec. Order 13526 § 1.2(a)(2). The unauthorized disclosure of information classified at the "CONFIDENTIAL" level ("C"), by definition, "reasonably could be expected to cause damage to the national security" of the United States. Exec. Order 13526 § 1.2(a)(3).

11. Sensitive Compartmented Information ("SCI") means classified information concerning or derived from intelligence sources, methods, or analytical processes, which is further restricted, with the requirement that it be handled within formal access control systems established by the Director of National Intelligence.

12. Classified information of any designation may be shared only with persons determined by an appropriate United States Government official to be eligible for access, and who possess a "need to know." Among other requirements, for a person to obtain a security clearance allowing that person access to classified United States Government information, that person is required to and must agree to properly protect classified information by not disclosing

such information to persons not entitled to receive it, by not unlawfully removing classified information from authorized storage facilities, and by not storing classified information in unauthorized locations. If a person is not eligible to receive classified information, classified information may not be disclosed to that person. In order for a foreign government to receive access to classified information, the originating United States agency must determine that such release is appropriate.

13. Pursuant to Executive Order 13526, classified information contained on automated information systems, including networks and telecommunications systems that collect, create, communicate, compute, disseminate, process, or store classified information must be maintained in a manner that: (1) prevents access by unauthorized persons; and (2) ensures the integrity of the information.

14. 32 C.F.R. Parts 2001 and 2003 regulate the handling of classified information. Specifically, 32 C.F.R. § 2001.43, titled "Storage," regulates the physical protection of classified information. This section prescribes that SECRET and TOP SECRET information "shall be stored in a GSA-approved security container, a vault built to Federal Standard (FHD STD) 832, or an open storage area constructed in accordance with § 2001.53." It also requires periodic inspection of the container and the use of an Intrusion Detection System, among other things.

Overview

15. The FBI is currently investigating the unauthorized disclosure of classified national defense information in connection with the posting of dozens of images of documents

on various public Internet sites, including U.S. social media platform, Discord.[1] Many of the documents depicted in these images bear classification markings, including "TOP SECRET" markings, which would serve to indicate the presence of U.S. Government classified information, including national defense information (the "Government Information").

16. As set forth in further detail below, JACK DOUGLAS TEIXEIRA is a current employee of the United States Air National Guard ("USANG") who possesses a security clearance at the TS//SCI level by virtue of his employment with USANG. TEIXEIRA is stationed at Otis Air National Guard Base in Massachusetts, where he has access to classified information systems.

17. As described further below, there is probable cause to believe that TEIXEIRA posted Government Information onto a specific Discord server from approximately December 2022 to March 2023. Specifically, there is probable cause to believe that TEIXEIRA uploaded an image of a classified document (the "Government Document") to a specific server on Discord ("SERVER 1") using a particular username associated with TEIXEIRA. As described in further detail below, the user identification number for the subject account is [redacted]; ("SUBJECT ACCOUNT 1").

18. The Government Document describes the status of the Russia-Ukraine conflict, including troop movements, on a particular date. The Government Document is based on

[1] Discord is a VOIP and instant messaging social platform. Users of Discord have the ability to communicate with voice calls, video calls, text messaging, and can post media and files in private chats or as part of communities called "servers." A Discord server is a collection of persistent chat room and voice channels, some of which can only be accessed via invitation from a current member.

sensitive U.S. intelligence, gathered through classified sources and methods, and contains national defense information. A subject matter expert has confirmed that the Government Document is classified at the TS//SCI level.

19. In addition, after the Government Information was posted on SERVER 1, another SERVER 1 user using a different subject account with user ID [redacted] ("SUBJECT ACCOUNT 2") communicated with TEIXEIRA on Discord and reposted certain of the Government Information that TEIXEIRA had originally posted on a separate Discord server. Thus, there is probable cause to believe that evidence and information related to TEIXEIRA's original post to SERVER 1 from SUBJECT ACCOUNT 1 will be found in SUBJECT ACCOUNT 2.

20. As discussed more fully below, there is also probable cause to believe that TEIXEIRA created a separate Discord server on which the Government Information, to include classified information, was posted and/or discussed. Moreover, based on information Discord provided the Government, I also know that TEIXEIRA created a second username with user ID [redacted] ("SUBJECT ACCOUNT 3") and may have used SUBJECT ACCOUNT 3 (collectively, with SUBJECT ACCOUNT 1 and SUBJECT ACCOUNT 2, the "SUBJECT ACCOUNTS") to communicate on the new Discord server about the Government Information.

BACKGROUND

Discord

21. In my training and experience, Discord is a proprietary freeware voice over Internet protocol (VoIP) application for gaming and other online communities. The Discord client was built on the Electron framework using web technologies, which allows it to be multi-platform and run on personal computers and websites. The Discord application has services such

as free voice chat servers for users and dedicated server infrastructure, video calling and screen sharing, direct calling, instant messaging, videoconferences, and GameBridge API2 that allows game developers to support integration with Discord within games. Discord users can create a "server" for free and then invite other users to join the server in order to communicate with another user. A server can be configured as public, meaning anyone can join, or it can be configured to be private, in which case an invitation is required to join.

22. Discord users are able to create and maintain a friends list, participate in multiple servers or communication channels, and set their current status indicator to appear online, away, or invisible to other users. Discord servers can have multiple text-based and voice channels, both public and private. Text messages sent in these channels are persistent, stay visible, and are stored indefinitely. Users are able to communicate in only one channel at a time but can easily navigate between channels. Discord users are able to direct message, or private message to other Discord users. Discord users are able to view what game their Discord friends and other Discord server members are playing.

23. During the registration process for a Discord account, Discord asks subscribers to provide basic client information to include username and email address. Additionally, other online applications like Steam, Facebook, Spotify, Twitter, and the Xbox platform can be connected to a user's Discord account. Discord can be used from within a web browser, can be installed on a Windows, Mac, or Linux computer, or can be installed on an Apple iOS or

---

[2] API is Application Programming Interface and it enables communication between two applications. By using this interface, two applications can interact with each other, share rules, specifications, data, and settings.

Android mobile device. Discord has an optional paid version called "Discord Nitro" that provides a user with additional features. Therefore, the computers of Discord likely contain information concerning a user's account and their use of Discord services and possibly other connected services, such as account access information, email information, and account application and payment information. Discord also assigns a user identification number to each account. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify and locate the account user(s).

24. In my training and experience, service providers like Discord typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of login (i.e. session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website) and other log files that reflect usage of the account. In addition, service providers often have records of the IP address[3] used to register the account and the IP addresses associated with particular logins to and activity

[3] An IP address is a unique numeric address used by computers on the Internet. There are two types of IP addresses used on the Internet today. The IPv4 address uses 32 bits and looks like a series of four numbers, each in the range from 0-255, separated by periods - for example 123.4.56.78. Due to the growth of the Internet, the creation of additional IP addresses was needed; therefore, a new version of IP called 1Pv6, uses 128 bits for IP addresses - for example 2610:0020:6Fl5:0015:0000:0000:0000:0027, or its abbreviated form of 2610:20:6Fl5:15::27. Every computer connected to the Internet must be assigned an IP address so that Internet traffic may be directed properly from its source to its destination. Each IP address is uniquely assigned to a single connected device at any single point in time.

on the account. Because every device that connects to the Internet must use an IP address, IP addresses can help identify which computers or other devices were used to access the account.

25. In some cases, Discord users may communicate directly with Discord about issues relating to their account, such as technical problems, billing inquiries, or complaints from other users. Social networking providers like Discord typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications.

26. The computers or servers of Discord are likely to contain all the material just described, including stored electronic communications and information concerning subscribers and their use of Discord, such as account access information, transaction information, and account activation.

27. The above-identified information stored at Discord may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, the information stored by the provider in connection with the SUBJECT ACCOUNTS can indicate who has used or controlled the accounts or an associated account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

28. For example, email communications, contacts lists, and images sent (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the account at a relevant time. Further, information maintained by a provider can show how and when the account was accessed or used. For instance, it may allow investigators to understand

the chronological context of account access, and events relating to the crime under investigation. This "timeline" information may tend to either inculpate or exculpate the account user or allow the United States to identify that individual. In addition, providers like Discord often log the IP addresses from which users accessed the account along with the time and date. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the account access and use relating to the crime(s) under investigation. This geographic and timeline information may tend to either inculpate or exculpate the account user. Additionally, information stored at the user's account may further indicate the geographic location of the account user at a particular time (e.g., location information integrated into an image or video sent via email). Lastly, stored electronic data may provide relevant insight into the account owner's state of mind as it relates to the offense(s) under investigation. For example, this stored data may indicate the owner's motive and intent to commit a crime (e.g., communications relating to the crime), or consciousness of guilt (e.g., deleting data in an effort to conceal them from law enforcement).[4]

29. Based on my training and experience, I also know that evidence of who controlled, used, and/or created the SUBJECT ACCOUNTS may be found within the user-generated content created or stored by the subscriber. This type of evidence includes, for example, personal correspondence, personal photographs, purchase receipts, contact information,

[4] At times, internet services providers such as Discord can and do change the details and functionality of the services they offer. While the information in this section is true and accurate to the best of my knowledge and belief, I have not specifically reviewed every detail of the above-described services in connection with submitting this application for a search warrant. Instead, I rely upon my training and experience, and the training and experience of others, to set forth the foregoing description for the Court.

travel itineraries, and other content that can be uniquely connected to a specific, identifiable person or group. In addition, based on my training and experience, I know that this type of user-generated content can provide crucial identification evidence, whether or not it was generated close in time to the offenses under investigation. This is true for at least two reasons. First, people that commit crimes involving electronic accounts typically try to hide their identities, and many people are more disciplined in that regard right before (and right after) committing a particular crime. Second, earlier-generated content may be quite valuable because criminals typically improve their tradecraft over time. That is to say, criminals typically learn how to better separate their personal activity from their criminal activity, and they typically become more disciplined about maintaining that separation, as they become more experienced. Finally, because accounts like the SUBJECT ACCOUNTS do not typically change hands on a frequent basis, identification evidence from one period can still be relevant to establishing the identity of the account user during a different, and even far-removed, period of time.

TEIXEIRA's Background

30. Since May 2022, TEIXEIRA has been serving as an E-3/Airman First Class in the USANG and is stationed at Otis Air National Guard Base. TEIXEIRA enlisted in the Air National Guard in September 2019 as an E-1 rank. As of February 2023, TEIXEIRA's title was Cyber Defense Operations Journeyman.

31. As required for this position, TEIXEIRA holds a Top Secret security clearance, which was granted in 2021. Based on my training and experience, I know that to acquire his security clearance, TEIXEIRA would have signed a lifetime, binding non-disclosure agreement in which he would have had to acknowledge that the unauthorized disclosure of protected information could result in criminal charges.

32. In addition to TEIXEIRA's Top Secret clearance, he maintained sensitive compartmented access to other highly classified programs. He has also had this access since 2021.

33. On or about April 13, 2023, TEIXEIRA was arrested by the FBI after he exited [redacted]. According to Discord, which provided subscriber information related to SUBJECT ACCOUNT 1, SUBJECT ACCOUNT 1 was subscribed to by "Jack Teixeira" with a billing address of "[redacted]".[5] As a result, there is probable cause to believe that TEIXEIRA is the user of SUBJECT ACCOUNT 1.

TEIXEIRA Transmits National Defense Information on Discord

34. On or about April 10, 2023, the FBI interviewed the user of SUBJECT ACCOUNT 2, who was also a member of SERVER 1. According to the user of SUBJECT ACCOUNT 2, TEIXEIRA, the user of SUBJECT ACCOUNT 1, began posting purportedly classified information on Discord on or about December 2022 on SERVER 1, identified by guild ID [redacted] and channel ID [redacted]. According to the user of SUBJECT ACCOUNT 2, SUBJECT ACCOUNT 1 was the administrator of SERVER 1.

35. SERVER 1 had approximately 50 members, and the user of SUBJECT ACCOUNT 2 indicated that the purpose of SERVER 1 was to discuss geopolitical affairs and current and historical wars.

36. According to the user of SUBJECT ACCOUNT 2, an individual using SUBJECT ACCOUNT 1 initially posted the Government Information on SERVER 1 as paragraphs of text.

---

[5] The zip code of [redacted].

However, in or around January 2023, SUBJECT ACCOUNT 1 began posting photographs of documents on SERVER 1 that contained what appeared to be classification markings on official U.S. Government documents.

37. According to the user of SUBJECT ACCOUNT 2, one of the documents that was posted on SERVER 1 by TEIXIERA via SUBJECT ACCOUNT 1 was the Government Document which, as noted above, described the status of the Russia-Ukraine conflict, including troop movements, on a particular date. The Government Document, which was accessible to TEIXEIRA by virtue of his employment with USANG, is based on sensitive U.S. intelligence, gathered through classified sources and methods, and contains national defense information. An Original Classification Authority has confirmed that the Government Document is classified at the TS//SCI level. As described above, TOP SECRET information "reasonably could be expected to cause exceptionally grave damage to the national security" of the United States. Exec. Order 13526 § 1.2(a)(1), 75 Fed. Reg. 707, 707–08 (Jan. 5, 2010).

38. According to a U.S. Government Agency, which has access to logs of certain documents TEIXEIRA accessed, TEIXEIRA accessed the Government Document in February 2023, approximately one day before the user of SUBJECT ACCOUNT 2 reposted the information on a separate Internet website. The user of SUBJECT ACCOUNT 2 told the FBI that the information he reposted was originally posted on SERVER 1 by the individual using SUBJECT ACCOUNT 1. The user of SUBJECT ACCOUNT 2 told the FBI that he also reposted classified information from SERVER 1 on a separate Discord server.

39. According to the user of SUBJECT ACCOUNT 2, he spoke to TEIXEIRA, who was using SUBJECT ACCOUNT 1, at various times using a video chat application, voice calls, and the chat function on SERVER 1. The user of SUBJECT ACCOUNT 2 stated that the

individual posting under SUBJECT ACCOUNT 1 identified himself as "Jack," appeared to reside in Massachusetts, and claimed that he was in the USANG. The user of SUBJECT ACCOUNT 2 further described the individual as a white male who was clean-cut and between 20 and 30 years old.

40. On April 13, 2023, the user of SUBJECT ACCOUNT 2 identified TEIXEIRA's Registry of Motor Vehicles photo from a photo lineup, and identified TEIXEIRA as the individual that he communicated with via SUBJECT ACCOUNT 2 on multiple occasions by video, voice, and computer chats on Discord, who used SUBJECT ACCOUNT 1, and who admitted to posting documents on SERVER 1.

41. On or about April 12, 2023, Discord provided the FBI with records pursuant to legal process, which included records related to SUBJECT ACCOUNT 2's Discord Account as well as the subscriber information for SUBJECT ACCOUNT 1. The records for SUBJECT ACCOUNT 1 revealed that TEIXEIRA was the administrator of SERVER 1, which is where SUBJECT ACCOUNT 2 first saw the Government Information posted by TEIXEIRA using SUBJECT ACCOUNT 1. Those records show that the username of SUBJECT ACCOUNT 1 was TEIXEIRA's username and the billing name for SUBJECT ACCOUNT 1 was Jack Teixeira, as described above. Those records also show that the User ID associated with SUBJECT ACCOUNT 2 is [redacted].

42. According to information from Discord, TEIXEIRA also created a second username with user ID [redacted] (SUBJECT ACCOUNT 3). The email associated with that account begins with "jdt," the initials associated with JACK DOUGLAS TEIXEIRA. According to the records from Discord, although SUBJECT ACCOUNT 3 was registered in March 2022, the first use of SUBJECT ACCOUNT 3 did not occur until February 20, 2023, and

regular use of SUBJECT ACCOUNT 3 did not begin until April 7, 2023. The IP address associated with the first login to SUBJECT ACCOUNT 3 is the same IP address regularly associated with SUBJECT ACCOUNT 1 and which was used as recently as April 6, 2023 by SUBJECT ACCOUNT 1. A second IP address associated with SUBJECT ACCOUNT 3 was also associated with SUBJECT ACCOUNT 1 and was used as recently as April 8, 2023 by SUBJECT ACCOUNT 3. In light of the above, I have reason to believe that SUBJECT ACCOUNT 3 is also associated with TEIXEIRA.

43. Moreover, I have reviewed open source reporting, which suggests that after the Government Information had been more widely disseminated and received media attention, TEIXEIRA moved SERVER 1 to a different server on Discord to continue to communicate with the users of SERVER 1. According to that reporting, TEIXEIRA encouraged the users of SERVER 1 to "delete any information that could possibly relate to him." As of April 7, 2023, when regular use of SUBJECT ACCOUNT 3 began, there was widespread media reports regarding leaks of purported government documents. Accordingly, I have reason to believe that TEIXEIRA may have used SUBJECT ACCOUNT 3 to continue to communicate on Discord regarding the Government Information.

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

44. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Discord to disclose to the government copies of the records and other information (including the content of communications) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

REQUEST TO SEAL AND PRECLUDE NOTICE TO SUBSCRIBERS

45. I request that this application, the warrant, the order, and any related papers be sealed by the Court until such time as the Court directs otherwise. I further request that, pursuant to 18 U.S.C. § 2705(b), the Court order Discord not to notify any person (including the subscribers or customers to which the materials relate) of the existence of this application, the warrant, or the execution of the warrant for a period of one year, unless the Court extends such period under 18 U.S.C. § 2705(b). Such an order is justified because notification of the application, the warrant, or the execution of the warrant could seriously jeopardize the ongoing investigation by giving any suspects an opportunity to destroy evidence, notify confederates, intimidate witnesses, or flee from prosecution.

CONCLUSION

46. Based on the forgoing, I request that the Court issue the proposed search warrant.

47. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

48. The government will execute this warrant by serving the warrant on Discord.

49. Because the warrant will be served on Discord, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

Respectfully submitted,

Victoria Horne
Special Agent
Federal Bureau of Investigation

~~Subscribed and~~ sworn to telephonically on Apr 17, 2023, 2023

10:25 p.m.

David H. Hennessy
UNITED STATES MAGISTRATE JUDGE